ISSN 2090-3359 (Print)
ISSN 2090-3367 (Online)

Advances in Decision Sciences

Volume 27
Issue 3
September 2023

亞洲大學
ASIA UNIVERSITY

Published by Asia University, Taiwan

Novel Standard Polynomial as New Mathematical Basis for Digital Information Encryption Process

Wisam Abed Shukur

Department of Computer Science, University of Baghdad, College of Education for Pure Sciences, Ibn Al–Haitham, Baghdad, Iraq

Email: wisam.a.s@ihcoedu.uobaghdad.edu.iq

Zaid M. Jawad Kubba

Department of Computer Science, University of Baghdad, College of Education for Pure Sciences, Ibn Al–Haitham, Baghdad, Iraq

***Corresponding author* Email:** zaidkubba@colaw.uobaghdad.edu.iq

Saif Saad Ahmed

Department of Computer Science, University of Baghdad, College of Education for Pure Sciences, Ibn Al–Haitham, Baghdad, Iraq

Email: Saif.S.a@ihcoedu.uobaghdad.edu.iq

Received: September 21, 2023; First Revision: September 29, 2023

Last Revision: November 30, 2023; Accepted: December 10, 2023

Published: January 17, 2024

Abstract

Objective: The proposed approach is based on producing new irreducible polynomials that help reduce the drawbacks of traditional cryptosystems. This work demonstrates the proposed model's efficiency and applicability, which could help researchers and practitioners investigate the proposed model in different cryptosystems and other related systems. In addition, the structure of the proposed polynomial function can be implemented in different cryptosystems with lightweight processing. The primary objective of this work is to present an efficient irreducible polynomial equation that can be implemented with lightweight cryptosystems.

Methodology: The proposed work is based on computing an irreducible polynomial, which is no more than two power multiplications. The structure of the proposed irreducible polynomial is carried out by using the exhaustive search approach and experiment. The mathematical function of the new standard polynomial is applied to generate a vital sequence of the proposed cipher algorithm.

Various quantitative and statistical methods are applied to decision sciences at the individual and population levels.

Findings-. The generated sequence keys are examined and analyzed using different statistical tests. The analysis output showed a significant random behavior of the generated sequence keys of the proposed cipher algorithm compared with the original cipher algorithm.

Novelty: This work considers a new approach based on the results, the proposed model's originality, and uniqueness in the literature. This work introduced a new standard polynomial function for a lightweight cipher algorithm that was implemented to develop a new lightweight cryptosystem for the digital information encryption process. The current cryptosystems suffer from computational complexity, which exceeds the quadratic power multiplication. Thus, this work presented a new design of the digital information encryption process, which contributed to solving traditional cryptosystems' cost and performance problems.

Keywords*:* Irreducible Polynomial, Lightweight Cryptosystem, Encryption, Data Security

JEL Codes: C02; C60; G32

1. Introduction

Mathematical models are the primary basis of every issue that can be solved based on different equations. The complexity of the cryptosystem can be achieved by increasing the level of the randomness process of key generating (Kubba & Hoomod, 2020; Shukur, et al., 2023). The main idea of the randomness approach for cipher algorithms of sensitive information is based on producing new keys in each iteration of the encryption process (Shukur, et al., 2021). From the security concern of complexity, performance, and independence, the keys generation should be high randomness of a candidate cipher algorithm (Lu, et al., 2023).

Diverse cipher algorithms are designed and developed to achieve security matters for digital information (Abdullatif, et al. 2018; Ali, et al., 2022). In contrast, most cipher algorithms encounter a significant obstacle during the encryption process: the high computational cost complexity (Kubba & Hoomod, 2019). Thus, digital information encryption process applications needed a new and efficient approach suited for such cryptosystems (Abdullatif, et al., 2019; Akif, et al., 2021). In addition, most cipher algorithms' simple and low computational complexity should consider the trade-off between the computational cost and performance. Furthermore, the characteristics of an efficient cryptosystem should involve the execution time and randomness of the system against the cryptanalysis (Kubba & Hoomod, 2020). Different cipher algorithms are considered lightweight for procedures requiring low computational cost (Ghazi, et al., 2021). The mathematical model of such algorithms is considered simple, and the encryption processes require a small execution time for the algorithm iterations. However, such cryptosystems still require more development and enhancement with a new mathematical model for producing an efficient encryption process.

Therefore, a new standard model should have characteristics such as easy to evaluate and validate the original issue. The characteristically of such a model can be built via a relatively slight number of variables and constants that formalize and estimate the input-output relation of the original issues under study. In addition, the standard model should consider the low cost of estimating and processing the uncertainty of the original seeds (Lüthen, et al., 2021).

Irreducible polynomials, such as cryptosystems and other science and technology systems, play a crucial role in information technology. Despite this, Irreducible polynomial functions are still considered complex models, and searching for a simple irreducible polynomial is still a significant concern. Developed cryptosystems of applied science have worked on adapting polynomials of the highest complex degree but also processed at a high cost. Hence, the core problem is that most known algorithms for the irreducible polynomials are inherent in quadratic modeling complexity. Moreover, adapting quadratic function required high costs of resources for construction and increased significantly with the degree of irreducible polynomials complexity (Beletsky, 2021).

Therefore, this work will present a new standard polynomial function to reduce and solve the complexity of the digital information encryption process. In addition, a variety of quantitative and statistical would be applied to decision sciences at the individual and population levels.

This study is organized as follows. Section 2 describes the theoretical background for categorizing the polynomial basics and the literature frameworks. Section 3 proposes an irreducible polynomials model and a proposed cryptosystem. Section 4 discusses the results, and finally, Section 5 explores the conclusions of the work.

2. Theoretical Basis

The polynomial function is one of the most widely applied computational models in computer science. Polynomial is a mathematical expression including constants and variables with different powers multiplied by coefficients. The functions are designed based on basic operations: addition, subtraction, multiplication, and division (Weisstein, 2002). A proposed post-quantum method is developed for public key cryptosystems based on polynomial equations over a non-commutative algebraic method (Hecht, 2020). Some studies examined polynomial equations over the Galois field (GF) and can design a robust key sequence module that would transform the essential seed of arbitrary length to a specific number of defined round keys in parallel l (Liu & Niu, 2022).

The core perception of information theory is the complexity that shapes the variants and imagines the object in more ingredients required to construct, create, or derive it. Recent works have examined the complexity as distant in computer science and applied sciences for developing systems in various areas (Mück & Yang, 2022). The understanding of complexity can be defined in terms of polynomial equations (Devi, et al., 2022). In mathematics, polynomial equations are considered as a family of any two different polynomials representation in a similar sequence to each other below some internal product operation (Kyriienko, et al., 2021). One of the important representations related to polynomial functions of degree n in one variable x with constants through a finite GF(p) is the illustration of the category of factorization of the polynomial n(x) (Brochero-Martinez, et al., 2019). GF arithmetic is holding a finite number of variables conflicting with calculation in a field of rational numbers. In addition, GF is implemented in various applications, including in classical encryption systems such as block cipher, cryptography algorithms, keys scheduling, and the design of applied sciences. A simple polynomials equation over a GF of uninformed features can be formed by the product of two variants of irreducible polynomials with a previously unidentified degree.

Some theoretical studies proposed an efficient computational model of constricting and developing functions for factorizing the degree of a standard polynomial (Kumbinarasaiah, 2021). The efficient model should be factored in to provide minimum computational complexity (Bielenova, et al., 2022; Kuang, et al., 2022). Thus, there is a need to construct and design a reduced polynomial function for solving the computational complexity, which involves two equations with unknown degrees of factors (Beletsky, 2022).

The theoretical basis for representing the standard irreducible polynomials can be shown in two forms. The first form is based on algebraic, as illustrated in function 1, and consists of a group of coefficients α and x of the irreducible polynomial.

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_k x^k + \ldots + a_1 x + a_0. \quad (1)$$

The second form is mainly based on the vector formula, a group of coefficients α of the irreducible polynomial consisting of zero coefficients to the absent monomials of series systems, as illustrated in function 2. The second form is shown as a problem of the existence of monic irreducible polynomials through successive zero coefficients.

$$f_n = a_n a_{n-1} \dots a_k \dots a_1 a_0. \quad (2)$$

Thus, new irreducible polynomials will be presented in this work to reduce and solve the complexity of factorizing the degree of polynomial equations.

3. The Proposed Irreducible Polynomials

Below are the primary model of the novel standard polynomials and the proven tables of how it calculated and satisfied the main conditions of the Irreducible Polynomial states.
Using the Gaussian Field (GF) of two bits, the Irreducible Polynomial states are considered as [00, 01, 10, 11]. They will be calculated based on the following multiplication operation of GF, as shown in Table 1.

Table 1. The multiplication operation of GF $(2)^2$

Θ	**1**	**x**	**x+1**
1	1	x	x+1
x	x	x^2 (*)	x^2 + x (*)
x+1	x+1	x^2 + x (*)	x^2 +2x +1 (*)

Table 1 represents the distribution of x variables and constants of the proposed Irreducible Polynomials. From table 1, the row and column of element Zero do not exist in our Computations. Thus, the terms in Table 1 are constructed based on [01, 10, 11] as the sequence elements [1, x, x+1]. The terms obtained via the multiplication operations of GF in Table 1 were considered into two categories. The first terms are constants, which are [1, x, x+1] and are considered the primary keys of the Irreducible Polynomials. The second terms, equal to or exceeding x2, should be excluded from the table where the primary condition, Irreducible Polynomials, should contain elements less than the proposed GF function, where considered as GF(2)2 in our proposed function. Therefore, the terms in Table 1 that are considered out of the proposed irreducible polynomials are denoted with a unique mark (*). However, these terms are considered the problem of computing the Irreducible Polynomials, and the proposed work is based on solving this issue and building a new model for the standard polynomial functions.

3.1 The New Model of The Standard Polynomial Functions

Before starting to build our model, the terms of Table 1 are considered the critical keys that should be processed to find the solution of the proposed irreducible polynomials. To solve the problem

above, we inserted only one integer (+1) for each term of Table 1, as shown in the following polynomial equations:

$$X^2 + 1, \quad (3)$$

$$X^2 + X + 1, \quad (4)$$

$$X^2 + X + 1, \quad (5)$$

$$X^2 + 2X + 1 + 1. \quad (6)$$

The proposed four equations above are determined based on Table 1, where each irreducible polynomial equation is denoted by the mark (*) and rebuilt by adding +1 for each formula, as shown above. In this work, we proposed a new standard irreducible polynomial equation that satisfies the required conditions, such as the occurrence of each polynomial term must be equal, that is:

$$X^2 + X + 2. \quad (7)$$

To prove the success of applying the proposed standard irreducible Polynomial, the devising operation for all states will be applied as follows:

$$(X^2 + X + 2) / (X^2 + 1) = X + 1, \quad (8)$$

$$(X^2 + X + 2) / (X^2 + X + 1) = 1, \quad (9)$$

$$(X^2 + X + 2) / (X^2 + X + 1) = 1, \quad (10)$$

$$(X^2 + X + 2) / (X^2 + 2X + 2) = X. \quad (11)$$

Table 2. The final parameters and representation that satisfy the standard irreducible polynomial.

Θ	**1**	**x**	**x+1**
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

Table 2 illustrates the number of occurrences of each parameter of the proposed Irreducible Polynomials, which is circled by three parameters [1, x, x+1], and the number of occurrences is 3, 3, 3.

3.2 The Proposed Cryptosystem Based on New Mathematical Model

This section will introduce a proposed developed key generation based on a new standard polynomial function. The key generation of the LED-128 algorithm is proposed for enhancement based on irreducible polynomials. The new method of using a novel irreducible polynomial with the key generation of the suggested LED algorithm enhances the performance and keeps the computational cost at a minimum. Figure 1 displays the block diagram of the proposed key generation based on the new polynomial function implemented with Led algorithm operations.

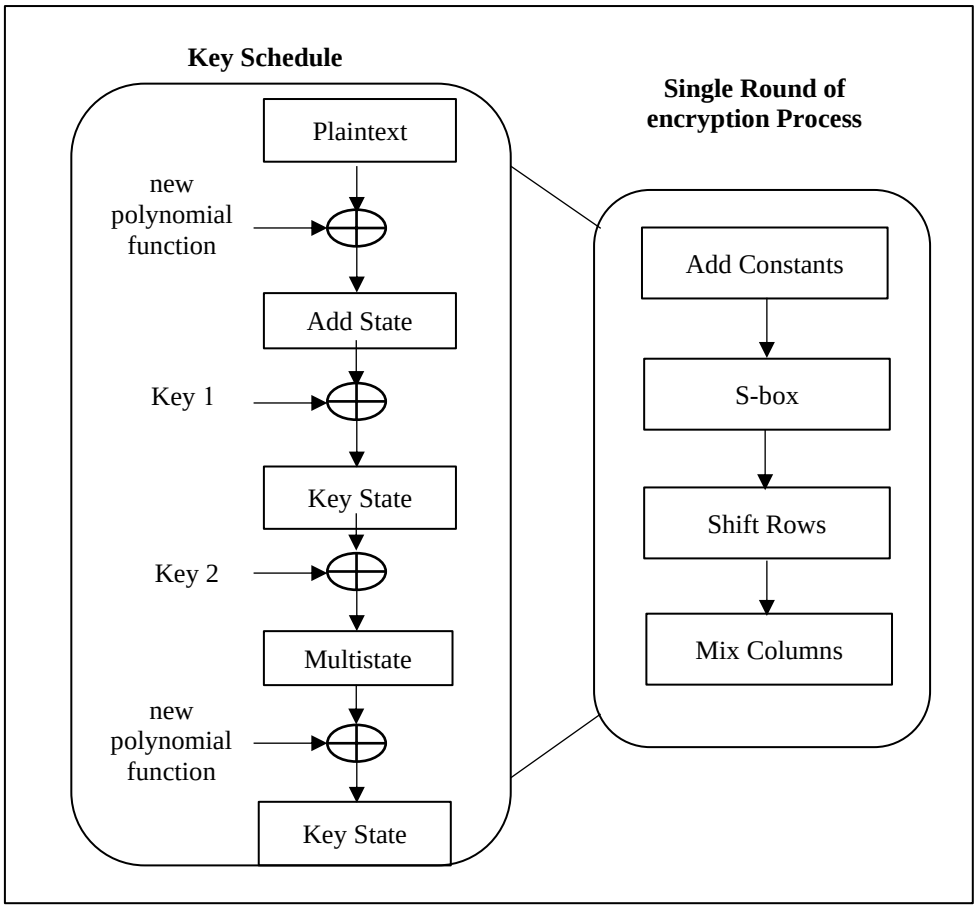

Figure 1. Block diagram of the suggested LED-128 algorithm.

The new standard polynomial function is implemented into the key generation of the suggested algorithm to minimize the gap between the complexity and the computational cost to present strong keys that add more robustness to the cipher LED algorithm. The proposed key schedule consists of 128 bits and is XORed with the plaintext input. The processes of key schedule states and the proposed encryption operations are illustrated in Figure 1. The key generation is produced based on the polynomial equation illustrated in section (3).

The generated keys are XORed with plaintext, and all key states are XORed with the round encryption operations. The round encryption operations contain four main layers: add constants, s-box, shift rows, and mix columns. The round operations of the LED algorithm will be XORed with the proposed key schedule at 32 rounds to produce a strong cipher text.

4. Results and Analysis

In this section, different analysis metrics and tests are implemented and programmed using Python language. The dataset used in the analysis is based on experiment text data of sensor devices collected through Raspberry Pi 3 device and stored as text files. The text of the data set is constructed as a block size of 64 bits. Various statistical metrics for examining the pseudorandom sequence of the keys generated through the proposed function produce efficient and good randomness properties of cipher algorithms (Hao & Min, 2014).

4.1 Analysis of NIST's Tests

The NIST statistical metrics were selected as the main prevalent, standard, and commonly applied for pseudorandom sequence tests (Zubkov & Serov, 2019). This work uses the 15 NIST metrics to compare the keys generated through the newly proposed polynomial function with the keys generated through the standard function. The experimented metrics are executed based on a critical sequence of 1000 bits size and divided into a block size of 64 bits (m = 64). Table 3 shows the results of the 15 NIST suite tests for the proposed Polynomial and Standard polynomial sequences.

Table 3. The 15 NIST metrics of the polynomial bits sequence.

Tests	**Standard Polynomial sequence**	**Proposed Polynomial sequence**
Frequency Analysis	0.002	0.36
Block Frequency Analysis	0.003	0.32
Cumulative Sums Analysis	0.012	0.46
Runs Analysis	0.02	0.23
Longest Run Analysis	0.003	0.34
Rank Analysis	0.05	0.05
FFT Analysis	0.01	0.34
Non-Overlapping Analysis	0.02	0.13
Overlapping Template	0.01	0.36
Universal Analysis	0.02	0.32
Approximate Entropy Analysis	0.01	0.23
Random Excursions Analysis	0.25	0.58
Random Excursions Variant	0.21	0.47
Serial Analysis	0.08	0.21
Linear Complexity Analysis	0.15	0.67

Table 3 explains 15 tests of the NIST statistics results from the standard and the proposed polynomial sequence. The result f is based on NIST metrics, and the randomness standard is measured via the key value (α) that thresholds the default value (0.01). A P-value represents each metric, and if the $P \geq 0.01$, then the sequence of bits should achieve the efficient randomness properties; otherwise, if $P < 0.01$, the sequence of bits does not pass the test, as illustrated in the following table. The results of the 15th matrices indicate that the proposed polynomial sequence obtained the highest P-values, and all tests were > 0.01. At the same time, the standard polynomial sequence gained less than the P-values of the tests as the proposed polynomial sequence. Therefore, the 15^{th} NIST test that examined the bits sequence showed a highly significant level of the generated

keys through the newly proposed polynomial equation and presented unpredictability properties that meet the requirements for a good cipher algorithm.

4.2 Correlation Coefficient Analysis

The correlation coefficient analysis (CCA) examines the link between two sequence bits, and the result of this test shows a degree that lies from -1 to +1. The degree considered within +1 represents a positive relation, while the degrees within -1 represent a negative relation. This metric is implemented broadly in cryptoanalysis and mathematical metrics for testing the reliability and robustness of a specific bits sequence in cryptosystems(Kamal & Tariq, 2019). This work examines the analysis based on Four different bit sequences, as shown in Table 4 below.

Table 4. The CCA of the standard and the proposed polynomial sequences.

Equations	State1	State2	State3	State4
Standard	0.23	0.14	0.03	0.31
proposed	-0.42	-0.21	-0.46	- 0.42

Table 4 examines four tests of the CCA from the standard and the proposed polynomial sequence. The CCA is computed based on the standard's relationship between two different polynomial sequences and the proposed method for Four states. The result shows that CCA degrees produced significant confusion and diffusion of the proposed polynomial equation.

In addition, table 5 shows the metrics results of the 15 NIST tests for the cipher text of the proposed LED cipher algorithm and the Standard LED algorithm.

Table 5. The 15 NIST test metrics results of the cipher text.

NIST Tests	Cipher text of LED algorithm	Cipher text of the proposed LED algorithm
Frequency Analysis	0.02	0.07
Block Frequency Analysis	0.15	0.25
Cumulative Sums Analysis	0.13	0.24
Runs Analysis	0.01	0.04
Longest Run Analysis	0.02	0.16
Rank Analysis	0.04	0.14
FFT Analysis	0.01	0.43
Non-Overlapping Analysis	0.24	0.57
Overlapping Template Analysis	0.01	0.23
Universal Analysis	0.23	0.48
Approximate Entropy Analysis	0.01	0.07
Random Excursions Analysis	0.43	0.64
Random Excursions Variant Analysis	0.12	0.26
Serial Analysis	0.07	0.12
Linear Complexity Analysis	0.25	0.38

Table 5 shows the 15 NIST test statistics results from the cipher text of the LED and proposed LED algorithms. The outcomes of the 15 metrics illustrate that the cipher text of the proposed LED algorithm gained the highest P-values, and all tests were > 0.01. At the same time, the cipher text of the LED algorithm obtained less than the P-values of the tests as proposed LED cipher text. Therefore, the 15 NIST tests showed a highly significant level of the generated keys through the proposed LED algorithm based on a new polynomial equation and produced unpredictability properties that meet the requirements for an efficient cipher algorithm.

5. Conclusion

This work presented a new polynomial equation for lightweight encryption algorithms. In addition, the proposed polynomial equation was implemented to enhance the key schedule of the LED cipher algorithm. The results indicated that the developed LED cipher algorithm based on the proposed polynomial equation has noticeable degrees of randomness compared to the standard cipher algorithm. The proposed approach is based on adding a new layer to the key generation of the LED algorithm, which produced a high confusion-diffusion of the cipher text. Thus, the proposed polynomial function is considered more efficient for lightweight cipher algorithms and produces high randomness behaviour which is proper for generating unbreakable keys of the Digital Information Encryption Process.

The measurement tools and statistical tests designate that the key schedule generated from the developed LED algorithms was more random and secure than the standard key schedule. This indicates that the proposed new polynomial equation strengthens the key schedule and produces efficient performance with the digital information encryption process.

This work occupies an essential trend in mathematical models and cryptography. Most mathematical models are complex, and their equivalent variants are complicated. Recently, nonlinear mathematical models have been conducted and developed to be connected with powerful digital encryption techniques. Thus, most recent works are based on polynomial equations and nonlinear mathematical maps. Hence, this work proposes a new standard polynomial that seems more efficient and can be implemented in different fields and systems, such as lightweight cipher algorithms. Various quantitative and statistical methods are applied to decision sciences at the individual and population levels. In contrast, previous works reported that some polynomial functions are considered complex and produce limitations in lightweight digital cryptosystems. The proposed standard polynomial is analyzed and tested based on mathematical and statistical tests, considered efficient for such cryptosystems. Moreover, various tests can be implemented to show the efficiency of the proposed polynomial equation in other fields. To extend the theory developed in this paper, one could apply some advanced econometrics, for example, portfolio optimization (Bai, et al., 2009; Li, et al., 2021), stochastic dominance (Bai, et al., 2011; Bai, et al., 2015), and causality (Bai, et al., 2018) to the theory developed in this paper and apply the theory developed in our paper to some important issues, for example, energy (W. Ali, et al., 2022; Arfaoui & Yousaf, 2022), bank (Abbas, et al., 2022; Nhan, et al., 2021; Noman, et al., 2023), capital market (Mahmood, et al., 2022; Suu, et al., 2021; Trang, et al., 2021), economic growth (Chang & Zhang, 2022; Chisadza & Biyase, 2023), and many others.

References

Abbas, F., Ali, S., & Wong, W. K. (2022). Impact of economic freedom and its subcomponents on commercial banks' risk-taking. Annals of Financial Economics, 17(03), 2250022.

Abdullatif, A. A., Abdullatif, F. A., & Naji, S. A. (2019). An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques. *Periodicals of Engineering and Natural Sciences, 7*(4), 1607-1617.

Abdullatif, F. A., Abdullatif, A. A., & al-Saffar, A. (2018). *Hiding techniques for dynamic encryption text based on corner point.* Paper presented at the Journal of Physics: Conference Series.

Akif, O. Z., Ali, S., Ali, R. S., & Farhan, A. K. (2021). A new pseudorandom bits generator based on a 2D-chaotic system and diffusion property. *Bulletin of Electrical Engineering and Informatics, 10*(3), 1580-1588.

Ali, R. S., Akif, O. Z., Jassim, S. A., Farhan, A. K., El-Kenawy, E.-S. M., Ibrahim, A., . . . Abdelhamid, A. A. (2022). Enhancement of the CAST Block Algorithm Based on Novel S-Box for Image Encryption. *Sensors, 22*(21), 8527.

Ali, W., Gohar, R., Chang, B. H., & Wong, W. K. (2022). Revisiting the impacts of globalization, renewable energy consumption, and economic growth on environmental quality in South Asia. Advances in Decision Sciences, 26(3), 1-23.

Arfaoui, N., & Yousaf, I. (2022). Impact of COVID-19 on volatility spillovers across international markets: evidence from VAR asymmetric BEKK GARCH model. Annals of Financial Economics, 17(01), 2250004.

Bai, Z., Liu, H., & Wong, W. K. (2009). Enhancement of the applicability of Markowitz's portfolio optimization by utilizing random matrix theory. Mathematical Finance: An International Journal of Mathematics, Statistics and Financial Economics, 19(4), 639-667.

Bai, Z. D., Hui, Y. C., Jiang, D. D., Lv, Z. H., Wong, W. K., & Zheng, S. H. (2018). A New Test of Multivariate Nonlinear Causality, PLoS ONE 13(1): e0185155. https://doi.org/10.1371/journal.pone.0185155

Bai, Z. D., Li, H., Liu, H. X., & Wong, W. K. (2011). Test statistics for prospect and Markowitz stochastic dominances with applications. Econometrics Journal, 122, 1-26.

Bai, Z. D., Li, H., McAleer, M., & Wong, W. K. (2015). Stochastic dominance statistics for risk averters and risk seekers: An analysis of stock preferences for USA and China. Quantitative Finance, 15(5), 889-900.

Beletsky, A. (2021). An Effective Algorithm for the Synthesis of Irreducible Polynomials over a Galois Fields of Arbitrary Characteristics. *WSEAS Transactions on Mathematics, 20*, 508-519.

Beletsky, A. (2022). Factorization of the Degree of Semisimple Polynomials Over the Galois Fields of Arbitrary Characteristics. *WSEAS Transactions on Mathematics, 21*, 160-172.

Bielenova, K., Nazarenko, H., & Vishnyakova, A. (2022). A sufficient condition for a complex polynomial to have only simple zeros and an analog of Hutchinson's theorem for real polynomials. *arXiv preprint arXiv:2207.08108*.

Brochero-Martinez, F., Reis, L., & Silva-Jesus, L. (2019). Factorization of composed polynomials and applications. *Discrete Mathematics, 342*(12), 111603.

Chang, F. H., & Zhang, L. (2022). Revisiting Inflation-Growth Nexus: An Endogenous Growth Model with Financial Frictions. Annals of Financial Economics, 17(01), 1-13.

Chisadza, C., & Biyase, M. (2023). Financial Development and Income Inequality: Evidence From Advanced, Emerging and Developing Economies. Annals of Financial Economics 18(01), 2241002

Devi, S., Mahajan, R., & Bagai, D. (2022). Low complexity design of bit parallel polynomial basis systolic multiplier using irreducible polynomials. *Egyptian Informatics Journal, 23*(1), 105-112.

Ghazi, A. B., Mahdi, O. A., & Abdulaziz, W. B. (2021). Lightweight route adjustment strategy for mobile sink wireless sensor networks. *Indonesian Journal of Electrical Engineering and Computer Science, 21*(1), 313-320.

Hao, L., & Min, L. (2014). Statistical tests and chaotic synchronization based pseudorandom number generator for string bit sequences with application to image encryption. *The European Physical Journal Special Topics, 223*(8), 1679-1697.

Hecht, P. (2020). PQC: R-Propping of Public-Key Cryptosystems Using Polynomials over Non-commutative Algebraic Extension Rings. *Cryptology ePrint Archive*.

Kamal, M., & Tariq, M. (2019). Light-weight security and blockchain based provenance for advanced metering infrastructure. *IEEE Access, 7*, 87345-87356.

Kuang, R., Perepechaenko, M., & Barbeau, M. (2022). A new post-quantum multivariate polynomial public key encapsulation algorithm. *Quantum Information Processing, 21*(10), 360.

Kubba, Z. M. J., & Hoomod, H. K. (2019). *A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System.* Paper presented at the 2019 First International Conference of Computer and Applied Sciences (CAS).

Kubba, Z. M. J., & Hoomod, H. K. (2020). *Modified PRESENT Encryption algorithm based on new 5D Chaotic system.* Paper presented at the IOP Conference Series: Materials Science and Engineering.

Kumbinarasaiah, S. (2021). Novel Functional Matrix Method using Standard Basis of Polynomial Linear Space. *International Journal of Applied and Computational Mathematics, 7*(4), 152.

Kyriienko, O., Paine, A. E., & Elfving, V. E. (2021). Solving nonlinear differential equations with differentiable quantum circuits. *Physical Review A, 103*(5), 052416.

Li, H., Bai, Z., Wong, W. K., & McAleer, M. (2021). Spectrally-Corrected Estimation for High-Dimensional Markowitz Mean-Variance Optimization, Econometrics and Statistics. 24, 133-150.

Liu, H., & Niu, Y. (2022). Cryptanalysis and designing chaos-based irreversible and parallel key expansion module over Galois field. *arXiv preprint arXiv:2212.05462*.

Lu, T., Chen, L., Han, J., Wang, Y., & Yu, K. (2023). RIS-assisted physical layer key generation by exploiting randomness from channel coefficients of reflecting elements and OFDM subcarriers. *Ad Hoc Networks, 138*, 103002.

Lüthen, N., Marelli, S., & Sudret, B. (2021). Sparse polynomial chaos expansions: Literature survey and benchmark. *SIAM/ASA Journal on Uncertainty Quantification, 9*(2), 593-649.

Mahmood, F., Shahzad, U., Nazakat, A., Ahmed, Z., Rjoub, H., & Wong, W. K. (2022). The nexus between cash conversion cycle, working capital finance, and firm performance: Evidence From Novel Machine Learning Approaches. Annals of Financial Economics, 17(02), 2250014.

Mück, W., & Yang, Y. (2022). Krylov complexity and orthogonal polynomials. *Nuclear Physics B*, *984*, 115948.

Nhan, D. T. T., Pho, K. H., ANH, D. T. V., & McAleer, M. (2021). Evaluating the efficiency of Vietnam banks using data envelopment analysis. Annals of Financial Economics, 16(02), 2150010.

Noman, M., Maydybura, A., Channa, K. A., Wong, W. K., & Chang, B. H. (2023). Impact of cashless bank payments on economic growth: Evidence from G7 countries. Advances in Decision Sciences, 27(1), 1-22.

Shukur, W. A., Badrulddin, A., & Nsaif, M. K. (2021). A proposed encryption technique of different texts using circular link lists. *Periodicals of Engineering and Natural Sciences, 9*(2), 1115-1123.

Shukur, W. A., Qurban, L. K., & Aljuboori, A. (2023). Digital Data Encryption Using a Proposed W-Method Based on AES and DES Algorithms. *Baghdad Science Journal*.

Suu, N. D., Tien, H. T., & Wong, W. K. (2021). The impact of capital structure and ownership on the performance of state enterprises after equitization: Evidence from Vietnam. Annals of Financial Economics, 16(02), 2150007.

Trang, L. N. T., Nhan, D. T. T., Hao, N. T. N., & Wong, W. K. (2021). Does Bank Liquidity Risk Lead To Bank's Operational Efficiency? A Study In Vietnam. Advances in Decision Sciences, 25(4), 46-88.

Weisstein, E. W. (2002). Polynomial. *https://mathworld.wolfram.com/*.

Zubkov, A. M., & Serov, A. A. (2019). Testing the NIST Statistical Test Suite on artificial pseudorandom sequences. Математические вопросы криптографии, 10(2), 89-96.